COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Joined By

THE 5-11 CAMPAIGN
THE ALA WASHINGTON OFFICE
THE AMERICAN CIVIL LIBERTIES UNION
THE AMERICAN POLICY CENTER
THE CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
THE CENTER FOR MEDIA AND DEMOCRACY
THE CYBER PRIVACY PROJECT
THE DEFENDING DISSENT FOUNDATION
THE ELECTRONIC FRONTIER FOUNDATION
THE LIBERTY COALITION
PRIVACY ACTIVISM
UNITED SIKHS

Privacy Expert

CHIP PITTS, Lecturer of Law at Stanford University Law School

to

THE DEPARTMENT OF HOMELAND SECURITY

"Notice of Privacy Act System of Records"

DHS-2011-0030

June 8, 2011

By a System of Records Notice ("SORN") published in the Federal Register on May 9, 2011, the Department of Homeland Security ("DHS") and the United States Citizenship and Immigration Services ("USCIS") proposed to establish a new system of records for the DHS E-Verify RIDE Program.[1] Pursuant to the DHS notice in the Federal Register, the Electronic Privacy Information Center ("EPIC") along with a coalition of privacy, consumer rights, and

[1] Notice of Privacy Act System of Records, 76 Fed. Reg. 26738 (May 9, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-05-09/html/2011-11291.htm [May 9, 2011 System of Records Notice]

civil rights organizations and individuals hereby submit these comments and recommendations to address the substantial privacy concerns raised by the proposal.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has particular interest in preserving privacy safeguards established by Congress, in the development of new information systems operated by the federal government.[2]

EPIC routinely analyzes and testifies about databases and verification programs used by federal entities. In Congressional testimony in 2005, EPIC Executive Director Rotenberg described some of the problems that would likely result from a poorly designed Employment Eligibility Verification System ("EEVS"), and some changes were made to EEVS based on

[2] *See*, *e.g.*, EPIC: Information Fusion Centers and Privacy, http://epic.org/privacy/fusion/; EPIC: EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill, http://epic.org/privacy/virginia_fusion/; Statement of Lillie Coney, EPIC Associate Director, to the Department of Homeland Security Data Privacy and Integrity Advisory Committee (Sept. 19, 2007), *available at* http://www. epic.org/privacy/fusion/fusion-dhs.pdf; Letter from Marc Rotenberg, EPIC Executive Director and John Verdi, EPIC Staff Counsel to Senate Committee on Homeland Security and Governmental Affairs and the Senate Subcommittee on State, Local, and Private Sector Preparedness and Integration (Apr. 17, 2008), *available at* http://www.epic.org/privacy/fusion/EPIC_ltr_Sen_Fusion_Ctrs.pdf; Press Release, EPIC, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008), *available at* http://epic.org/press/041108.html; Freedom of Information Act Request from John Verdi, Director, EPIC Open Government Project to Virginia State Police (Feb. 12, 2008), *available at* http://www. epic.org/privacy/fusion/VA_FOIA021208.pdf; Complaint, EPIC v. Martin and the Virginia Department of State Police (D. Va 2007), *available at* http://www. epic.org/privacy/fusion/VA_FOIA_lawsuit_032108.pdf; EPIC: Open Government, http://epic.org/open_gov/; EPIC: Spotlight on Surveillance: "National Network" of Fusion Centers Raises Specter of COINTELPRO, http://epic.org/privacy/surveillance/spotlight/0607/; EPIC: Privacy, http://epic.org/privacy/; Statement of Lillie Coney, EPIC Associate Director to ABA Conference, Computing and the Law: From Steps to Strides into the New Age (June 25-26, 2007), *available at* http://www. epic.org/epic/staff/coney/surveillance.pdf; Letter from EPIC, et. al to Representative Bennie G. Thompson, Chair, U.S. House of Representatives Committee on Homeland Security and Representative Peter T. King, Ranking Member, U.S. House of Representatives Committee on Homeland Security (Oct. 23, 2009), *available at* http://www. epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf; EPIC: EPIC Alert 15.10, "EPIC Prevails in Virginia Fusion Center FOIA Case," (May 16, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-May/000001.html; EPIC: EPIC Alert 14.19, "DHS Privacy Advisory Panel Holds Hearing on Fusion Center," (Sept. 20, 2007), http://epic.org/alert/EPIC_Alert_14.19.html; EPIC: "DHS Releases Fusion Center Privacy Impact Assessment," EPIC Alert 15.25 (Dec. 23, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-December/000017.html; EPIC: "Documents Reveal Federal Role In Fusion Center Secrecy," EPIC Alert 15.08 (Apr. 17, 2008), http://epic.org/alert/EPIC_Alert_15.08.html; EPIC: Department of Homeland Security Chief Privacy Office and Privacy, http://epic.org/privacy/dhs-cpo.html.

EPIC's recommendations.[3] Again in Congressional testimony in June 2007, EPIC urged Congress to strengthen privacy and security safeguards associated with the EEVS the underlying databases.[4] EPIC has analyzed flaws in such systems in a number of reports.[5] EPIC has also focused on employment verification systems as part of its "Spotlight on Surveillance" series.[6]

The 5-11 Campaign is a not-for-profit grassroots campaign set to repeal national identity laws, laws requiring data surveillance specific to identified persons and/or to fitfully stop all appropriations to implement national identity.

The ALA Washington Office was established in 1945 to represent libraries on Capitol Hill. The ALA was founded on October 6, 1876 during the Centennial Exposition in Philadelphia, It was created to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all. ALA Washington Office's current strategic plan, ALA Ahead to 2010, calls for continued work in the areas of Advocacy and Value of the Profession, Education, Public Policy and Standards, Building the Profession, Membership and Organizational Excellence.

The American Civil Liberties Union ("ACLU") is the nation's oldest and largest civil liberties organization with more than half a million members, countless additional supporters and

---

[3] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005," Before the Subcomm. on Immigration, Border Sec., and Claims, H. Comm on the Judiciary*, 109th Cong. (May 12, 2005), *available at* http://www.epic.org/privacy/ssn/51205.pdf.

[4] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on Employment Eligibility Verification Systems (EEVS) Before the Subcomm. on Social Sec., H. Comm on Ways & Means*, 110th Cong. (June 7, 2007), available at http://www.epic.org/privacy/ssn/eevs_test_060707.pdf.

[5] *See* EPIC, Social Security Numbers, http://epic.org/privacy/ssn/; EPIC, Secure Flight, http://www.epic.org/privacy/airtravel/secureflight.html; and EPIC, National ID Cards and the REAL ID Act, http://epic.org/privacy/id-cards/.

[6] *See* EPIC, *E-Verify System: DHS Changes Name, But Problems Remain for U.S. Workers* (July, 2007), http://epic.org/privacy/surveillance/spotlight/0707/default.html; EPIC, *National Employment Database Could Prevent Millions of Citizens From Obtaining Jobs* (May, 2007), http://epic.org/privacy/surveillance/spotlight/0507/default.html.

activists, and 53 affiliates across the country. It advocates for individual rights though litigation, lobbying, and public education on a broad array of issues. The ACLU monitors the interplay between cutting-edge technology and civil liberties, actively promoting responsible uses of technology that enhance privacy and freedom, while opposing those that undermine our freedoms and move us closer to a surveillance society.

The American Policy Center ("APC"), located in suburban Washington, D.C., is a privately funded, nonprofit, 501(c)(4), tax-exempt grassroots action and education foundation dedicated to the promotion of free enterprise and limited government regulations over commerce and individuals.

The Center for Financial Privacy and Human Rights ("CFPHR"), was founded in 2005 to defend privacy, civil liberties and market economics. The Center is a non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy Network, a non-governmental advocacy and research 501(c)(3) organization.

The Center for Media and Democracy is an independent, non-profit, non-partisan, public interest organization that focuses on investigating and countering spin by corporations, industry and government; informing and assisting grassroots action that promotes public health, economic justice, ecological sustainability, human rights, and democratic values; advancing transparency and media literacy to help people recognize the forces shaping the information they receive about important issues affecting their lives; and promoting "open content" media that enable people from all walks of life to "be the media" and help write the history of these times.

The Cyber Privacy Project Cyber Privacy Project is a non-partisan organization focusing on governmental intrusions against Fourth and Fifth Amendment rights of privacy, particularly

in government databanks and national identification schemes for voting, travel and work, and on medical confidentiality and patient consent.

The Defending Dissent Foundation ("DDF"), founded in 1960, is a national grassroots civil liberties organization working to protect and advance the right of dissent in the United States. DDF translates grassroots civil liberties concerns into national policy debate and action; and alerts grassroots activists when civil liberties are threatened; and educates the public, the press and policymakers about the important role dissent plays in a democracy.

The Electronic Frontier Foundation ("EFF") is a member-supported nonprofit civil liberties organization with more than 14,000 members worldwide, dedicated to the protection of citizens' online civil rights, privacy, and freedom of expression. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to promote balanced laws that foster innovation and empower consumers. EFF is located in San Francisco, California and has members in 67 countries throughout the world.

The Liberty Coalition works to help organize, support, and coordinate transpartisan public policy activities related to civil liberties and basic rights. We work in conjunction with groups of partner organizations that are interested in preserving the Bill of Rights, personal autonomy and individual privacy.

Privacy Activism is a non-profit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level. A key goal of the organization is to inform the public about the importance of privacy rights and the short and long-term consequences of losing them – either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience.

UNITED SIKHS is a U.N. affiliated, international non-profit, non-governmental, humanitarian relief, human development and advocacy organization, aimed at empowering those in need, especially disadvantaged and minority communities across the world. UNITED SIKHS seeks to fulfill its mission not only by informing, educating and uplifting fellow beings but also by participating in cross-cultural and social dialogues to ensure that the promises and benefits of democracy are realized by all.

Chip Pitts is an international attorney, investor/entrepreneur, and law educator who advises businesses on international, strategic, intellectual property, marketing, legal, and ethics matters. Formerly Chief Legal Officer of Nokia, Inc. and partner at a major global law firm, he currently serves on the board for Amnesty International USA and was the former board chair. He is a Lecturer in Law at Stanford University Law School and has taught at other law schools and universities. He is a frequent speaker, writer, and commentator on ethical globalization, human rights, and foreign affairs in national and international law journals, magazines, newspapers, and broadcast media.

I. Background of E-Verify

E-Verify is a national internet-based computer records system that effectively requires employers to verify the citizenship status of their current and prospective employees.[7] The Department uses the system to retain names, dates of birth, Social Security numbers ("SSNs"), and citizenship status for all individuals subject to review.[8] The Department retains all of this information for ten years.[9] Employers who use the system require their employees to provide

[7] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify Program Privacy Impact Assessment (May 4, 2010).
[8] *Id*. at 9.
[9] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify RIDE Privacy Impact Assessment Update 7 (May 6, 2011).

Social Security numbers, which employees are otherwise not required to provide.[10] In fact, despite the Social Security Administration's ("SSA") participation in the E-Verify system, the SSA has previously stated that "[r]epetitive use and disclosure of SSNs in organizational record keeping systems . . . multiplies the susceptibility of persons to potential identity theft."[11] Employers submit their employees' SSNs to the Department of Homeland Security, as well as other personal information the employee provides through a "Form I-9" questionnaire.[12]

The Department matches the information it receives against E-Verify's databases, populated with records from the SSA's "Numident" System.[13] The Numident master file is a record of personally identifying information ("PII") including name, date of birth, and SSN.[14] The information is provided to the government by SSN applicants on Form SS-5 "Application for a Social Security Number."[15] The Department also uses the E-Verify system to match employee information against any number of the twenty-one databases maintained by DHS and other federal agencies.[16] These additional databases contain signatures, fingerprints, photo images, immigration statuses, addresses, changes of address, prior visa issuances or refusals, and government benefit eligibility data.[17] In its System of Records Notice, the Department provides an example of database verification.[18] An employee who provides an "Alien Number" would trigger an agency search into the USCIS Central Index System ("CIS") and a photo match with

[10] May 9, 2011 System of Records Notice at 26739.
[11] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.
[12] May 9, 2011 System of Records Notice at 26739.
[13] May 9, 2011 System of Records Notice at 26739-40.
[14] SOCIAL SECURITY ADMINISTRATION, THE SOCIAL SECURITY ADMINISTRATION'S IMPLEMENTATION OF THE E-VERIFY PROGRAM FOR NEW HIRES, AUDIT REPORT A-03-09-29154, OFFICE OF THE INSPECTOR GENERAL N.2 (2010).
[15] *Id*.
[16] May 9, 2011 System of Records Notice at 26740. U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify Program Privacy Impact Assessment 20-24 (May 4, 2010)..
[17] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify Program Privacy Impact Assessment 20-24 (May 4, 2010)..
[18] May 9, 2011 System of Records Notice at 26740.

an Employment Authorization Document ("EAD") image.[19] If DHS concludes that its search through these databases "verif[ies] the employee's employment eligibility," the agency sends the employer an "Employment Authorized" notification.[20] If not, the employer receives a "Verification in Process" response, and the Department undertakes further review.[21]

The Department's current proposal would add a new E-Verify database against which to check employee information.[22] The new database would merge federal background check records with state driver license data sets. The agency proposes to use AAMVAnet, described in the SORN as a "secure framework." In 2006, the Department of Transportation stated that AAMVAnet is "based on outdated, 1980's-vintage technology."[23] If employees present their employers with state drivers' licenses or permits, or state identification cards for those who do not drive, the Department proposes to check the identification document against the new database of state motor vehicle records, which the agency proposes to aggregate through "voluntary" state participation.[24]

Only one state, Mississippi in 2009, has voluntarily granted E-Verify access to its residents' information.[25] Forty nine states have refused, likely on grounds EPIC identified in Congressional testimony regarding E-Verify: "[p]rivacy is better safeguarded by storing data in multiple, decentralized locations, and only when necessary."[26] As EPIC has highlighted in the

[19] *Id*.
[20] *Id*.
[21] *Id.*
[22] May 9, 2011 System of Records Notice.
[23] U.S. Dep't of Transp., FY 2006 E-Government Act Report (2007), available at http://www.dot.gov/webpoliciesnotices/dotegovactreport2006.htm.
[24] *Id.* at 26738.
[25] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify RIDE Privacy Impact Assessment Update 10 (May 6, 2011).
[26] Employment Eligibility Verification Systems (EEVS): Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 110th (2007) (statement of Marc Rotenberg, President, Electronic Privacy Information Center) at 4..

past, however, it is unclear what "voluntary" means in this context.[27] The Department's previous conduct in securing "voluntary" state participation raises serious questions. For example, after stating that the REAL ID Act is not a mandate, former DHS Secretary Chertoff elaborated that if a state did not comply "then the state cannot expect that those licenses will be accepted for federal purposes."[28] Non-complying states were warned that individuals would not be able to use the state-issued identification to board a commercial aircraft, for example.[29] Utah State Legislature's resolution opposing the Real ID Act recognized the mandatory nature in criticizing that the law "coerces states into doing the federal government's bidding by threatening to refuse noncomplying states' citizens the privileges and immunities enjoyed by other states' citizens."[30]

II. The Proposal Claims Privacy Act Exemptions for "Routine Uses" Premised on Insufficient Legal Authority

DHS will not confine the use of E-Verify data to the narrow purpose of employment eligibility, even though Congress constrained the agency's grant of authority to that purpose. The Department has founded all of its authority to expand E-Verify on legislation that only discusses employment eligibility confirmation: the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"). [31] Congress tailored IIRIRA to the implementation of "pilot programs of employment eligibility confirmation."[32] E-Verify is one such "pilot program" and participation is limited to employment verification of new hires.[33]

---

[27] *See* EPIC, *E-Verify System: DHS Changes Name, But Problems Remain for U.S. Workers* (July, 2007), http://epic.org/privacy/surveillance/spotlight/0707/default.html;
[28] *See* Elliot McLaughlin, Federal ID Plan Raises Privacy Concerns, *CNN* (Aug. 16, 2008), *available at* http://www.cnn.com/2007/POLITICS/08/16/real.id/index.html?iref=newssearch.
[29] Letter to Governor John Baldacci from Stewart Baker, DHS Assistant Secretary of Policy (Mar. 31, 2008) *available at* http://epic.org/privacy/id_cards/dhs_maine_033108.pdf.
[30] Utah State Legislature's Resolution Opposing REAL ID Act, http://le.utah.gov/~2007/bills/hbillenr/hr0002.htm
[31] May 9, 2011 System of Records Notice at 26741; IIRIRA, Pub. L. No. 104-208, div. C, tit. IV, subtit. A, 110 Stat. 3009-546, 3009-655 (codified at 8 U.S.C. § 1324a).
[32] IIRIRA § 401(a).
[33] See IIRIRA §§ 402(c)(2)(A), 403(a).

Despite clear legal constraints, the agency unlawfully claims three routine uses it believes are exempt from Privacy Act reporting requirements. The agency cites the Privacy Act exemption "for a routine use as designed in subsection (a)(7) of [Section 552a(b)(3)] and described under subsection (e)(4)(D) of [Section 552a(b)(3)]."[34] Subsection (a)(7) exempts disclosures that are "compatible with the purpose for which [a record] was collected."[35] In this case, the agency lists three routine uses that are completely unrelated to the purpose Congress authorized E-Verify to collect records.

First, the SORN claims E-Verify data "may also be used for law enforcement," followed by specified examples in parentheses, "(to prevent fraud and misuse of E-Verify, and to prevent discrimination and identity theft)."[36] It is important to note that the agency fails explicitly to commit to these parenthetical examples as legal limitations. Second, the agency seeks unfettered power to distribute E-Verify records both to public and private parties. The SORN contemplates routinely disclosing:

> all or a portion of the records or information contained in this system…to an appropriate Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation of enforcing or implementing a law, rule, regulation, or order . . .[37]

Again, the agency includes a non-exhaustive, and therefore non-binding, list of examples: " . . . where a record, either on its face or in conjunction with other information, incidates a violation of potential violation of the E-Verify program, which includes potential fraud discrimination, or employment based identity theft . . . "[38] Third, the agency reserves the right to disclose E-Verify data "to the news media and the public" with a vague exception

[34] May 9, 2011 System of Records Notice at 26744;
[35] 5 U.S.C. 552a(b)(3) (2001).
[36] May 9, 2011 System of Records Notice at 26741.
[37] *Id.* at 26744-5.
[38] *Id.* at 26745.

for any "particular case [that] would constitute an unwarranted invasion of personal privacy."[39]

The agency must maintain a narrow mission for the E-Verify system with clear oversight mechanisms and limiting guidelines. The agency previously committed to a "policy" stating that E-Verify records will "only be used for the employment eligibility purposes of the E-Verify Program or for purposes that directly support the program such as prevention of misuse and fraud, program analysis and outreach."[40] In light of apparent inconsistencies with that commitment, the agency should refocus on the following three questions, clarify its SORN, and then re-issue an amended Privacy Act Notice:

- Are law enforcement uses of E-Verify data restricted to purposes that "directly support the program" of employment eligibility?
- Are disclosures to governmental agencies outside of DHS restricted to purposes that "directly support the program" of employment eligibility?
- What factors, standards, and precedents inform the agency's definition of "unwarranted invasion of personal privacy"?

Clear, precise answers to these questions will enable the public to assess and comment upon the agency's decision to expand E-Verify, which will allow DHS to properly evaluate the agency's proposed information collection.

III. The Proposal Further Complicates E-Verify's Insufficient Recourse for Incorrect Records

The Department of Homeland Security seeks to expand a program that fails systematically to amend or correct inaccurate, irrelevant, untimely, and incomplete records. The rights of access and correction are central to the Privacy Act of 1974, which established the agency's duty to publish this SORN.[41] However, the Government Accountability Office

[39] *Id.*
[40] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify Program Privacy Impact Assessment 31 (May 4, 2010)..
[41] H.R. Rep. No. 93-1416, at 15 (1974); 5 U.S.C. § 552a.

("GAO") reported in December 2010 that subjects of incorrect E-Verify records face "formidable challenges in getting the inaccuracy or inconsistency corrected."[42] After interviewing senior E-Verify program officials and analyzing the agency's recordkeeping, GAO published its report "Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain."[43] The Director of Homeland Security and Justice Issues at the GAO testified to Congress that the agency "has not established mechanisms for employees to identify and access personal information maintained by DHS that may lead to an erroneous [tentative non-confirmation], or for E-Verify staff to correct such information."[44]

The SSA Audit of the Numident system points to one significant source of flawed verification. In 2006, the SSA reported that 3.1 percent of the 810 foreign-born U.S. citizens' Numident records the agency audited were misclassified.[45] The agency estimated that "17.8 million Numident records contain discrepancies that may result in incorrect [E-Verify] feedback to employers."[46] The agency concluded by alluding to the increase in agency workload "if even a portion of the estimated numberholders whose Numident records contained discrepancies were required to visit an SSA office to correct their information."[47] As the GAO states, the legal mechanism for correcting a Numident error in the E-Verify system might entail "separate Privacy Act requests" to agencies within DHS and to the SSA, "because each DHS component maintains its own data and

---

[42] *Id*.
[43] U.S. Govt. Accountability Office, Employment Verification: Fed. Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain, GAO-11-146 (2010).
[44] Employment Verification: Fed. Agencies Have Improved E-Verify, but Significant Challenges Remain: Hearing Before the Subcomm. on Immigration Policy and Enforcement of the H. Comm. on the Judiciary, 112th Cong. (2011) (statement of Richard M. Stana, Director, Homeland Security and Justice) at 7.
[45] Office of the Inspector Gen., U.S. Soc. Sec. Admin., Pub. No. A-08-06-26100, Congressional Response Report: Accuracy of the Social Security Administration's Numident File 9 (Dec. 2006), *available at* http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.
[46] *Id*. at 14
[47] *Id*. at 14.

has an independent office in charge of responding to Privacy Act requests."[48] The GAO stated that the average response time for Privacy Act requests to correct database information was "approximately 104 days."[49] Errors in state motor vehicle databases would be even more complicated, as the agency asserts that "the data in the system is owned by the organization that had the original authority to collect the data."[50]

Before expanding the E-Verify system to include state identification databases, it is essential for the agency to develop an effective system for meaningfully enforcing the right of data subjects to quickly correct government records pertaining to their right to employment.

IV. The Proposal Exposes New Information To An Environment With Demonstrated Security Failures

EPIC has previously explained to the agency that "[a]n all-inclusive database provides an appealing mark for thieves trying to create false identities for criminal activities."[51] The agency implicitly acknowledges this critique of its E-Verify system in the SORN itself, by explicitly contemplating that failure to properly secure the sensitive information E-Verify collects will result in:

> a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system of other system of programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information.[52]

---

[48] U.S. Govt. Accountability Office, Employment Verification: Fed. Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain, GAO-11-146 34 (2010).
[49] *Id*.
[50] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify RIDE Privacy Impact Assessment Update 3 N.3 (May 6, 2011).
[51] Employment Eligibility Verification Systems (EEVS): Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 110th (2007) (statement of Marc Rotenberg, President, Electronic Privacy Information Center) at 4.
[52] May 9, 2011 System of Records Notice at 26744.

The only apparent safeguard the agency has designed to account for this particular risk is an even more expansive claim of authority to further disclose sensitive information "to appropriate agencies, entities, and persons" in case of a major breach.[53] The agency also tacked a "Safeguards" section onto the final page of the SORN, asserting that "[r]ecords in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies."[54]

Multiple data breaches at the Department of Homeland Security over the last five years call into question the efficacy of these policies. In 2006, one hundred and fifty DHS computers were compromised by hackers "who sent an unknown quantity of information to a Chinese-language Web Site."[55] The intruders "used special software to crack a user account password for a network administrator who had privileges to modify key system files on thousands of computers on the DHS network."[56] In 2007, the Transportation Security Administration, a critical component of the DHS, lost the employment records of one hundred thousand federal employees.[57] The records contained the names, SSNs, DOBs, payroll history, and detailed bank information for every person the TSA hired between January 2002 and August 2005, including federal air marshals who fly undercover to help safeguard commercial aviation in the United States.[58] The agency has since taken down a website dedicated to the incident.[59] In

---

[53] *Id.*
[54] *Id.* at 26745.
[55] Ellen Nakashima and Brian Krebs, *Contractor Blamed in DHS Data Breaches*, WASH. POST., Sept. 24, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471_pf.html.
[56] *Id*.
[57] Press Release, U.S. Transp. Sec. Admin., Public Statement on Employee Data Security Incident (May 4, 2007), *available at* http://www.tsa.gov/press/happenings/050407_statement.shtm.
[58] Employment Eligibility Verification Systems (EEVS): Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 110th (2007) (statement of Marc Rotenberg, President, Electronic Privacy Information Center) at 2.

2010, government contractor KPMG LLP lost an unencrypted flash drive that "last observed in an unlocked conference room in the KPMG offices where it had been left at the end of the work day."[60] DHS reported that "numerous written policies to protect client data" were neither monitored nor enforced, and the employees handling the lost flash drive did not follow them. The records included names, SSNs, and bank routing and account numbers.[61]

Before expanding E-Verify, it is an essential that DHS improve its security measures and reduce the risk of lax practices that contribute to identity theft and financial fraud.

V. The Proposal to Expand E-Verify Approaches the National Identification System that Congress Explicitly Prohibited

Like the REAL ID Act, which attempted to standardize and coordinate federal and state records by requiring states to verify federal information before issuing identification,[62] the updated E-Verify system will query participating states' motor vehicle administration databases to verify information.[63] In establishing the Department of Homeland Security, Congress declared that "nothing in [the chapter pertaining to Homeland Security Organization] shall be construed to authorize the development of a national identification system or card."[64] Former Secretary of Homeland Security Tom Ridge reiterated that "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They

---

[59] Press Release, U.S. Transp. Sec. Admin., Public Statement on Employee Data Security Incident (May 4, 2007), *available at* http://www.tsa.gov/press/happenings/050407_statement.shtm. (follow "CLICK HERE For TSA'S website dedicated to the Employee Data Security Incident" link).
[60] DHS PRIVACY OFFICE, U.S. DEP'T OF HOMELAND SEC., OIG PRIVACY INCIDENT REPORT AND ASSESSMENT 1 (Feb. 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/priv-oig-privacy-incident-report-assessment-022011.pdf.
[61] *Id*.
[62] § 202
[63] May 9, 2011 System of Records Notice at 26740
[64] 6 U.S.C. § 554 (2006).

said there will be no national ID card."[65] Current Secretary Janet Napolitano has been working with state governors to mobilize complete repeal.[66] The System of Records Notice at issue contradicts these stated limitations by attempting to merge state and federal identification data to implement REAL ID Act's requirements under a new name.

DHS failed to restrict its use of the state-collected information to previously stated purposes for the REAL ID program, opening the door to broad usage. Title II of the REAL ID Act of 2005 established federal standards for state-issued drivers' licenses and identification cards,[67] replacing the former system of cooperation between federal and state officials to create standards.[68] While passed upon recommendation from the 9/11 Commission as an anti-terrorism measure,[69] DHS sought to employ the identification system for other purposes such as preventing illegal immigration and identity theft, noting that the agency could "kill three birds with one stone if we get ourselves on a path to a secure driver's license."[70] A number of states passed legislation refusing to aid federal implementation of REAL ID. [71]

Recognizing the multiple purposes contemplated by Real ID implementation, the Department of Homeland Security's Data Privacy and Integrity Advisory Committee cautioned that "[p]rivacy is best protected when information collected for a specified purpose is used

---

[65] Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University "Transatlantic Homeland Security Conference (Sep. 13, 2004), http://www.dhs.gov/xnews/speeches/speech_0206.shtm.

[66] HR 117 (110th Congress) REAL ID Repeal and Identification Security Enhancement Act of 2007; *Homeland Security Chief Seeks Repeal to REAL ID Act*, CNN (Apr. 22, 2009), *available at* http://articles.cnn.com/2009-04-22/politics/real.ID.debate_1_real-id-act-licenses-and-identification-cards-napolitano?_s=PM:POLITICS.

[67] REAL ID Act (Public Law § 202).

[68] REAL ID Act (Public Law § 207 – repealing Intelligence Reform and Terrorism Prevention Act of 2004)

[69] Final Rule (6 CFR pt. 37, p. 5273)

[70] Remarks by former Homeland Security Secretary Michael Chertoff at a Press Conference on REAL ID (Jan. 11, 2008), http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm

[71] *See* Elliot McLaughlin, Federal ID Plan Raises Privacy Concerns, *CNN* (Aug. 16, 2008), *available at* http://www.cnn.com/2007/POLITICS/08/16/real.id/index.html?iref=newssearch ("More than half the nation's state legislatures have passed or proposed legislation denouncing the plan, and some have penned bills expressly forbidding compliance.").

exclusively for that purpose."[72] This warning highlights a similar risk with the current proposal, which states that in addition to employment verification, the proposed new collection of information "may also be used" for law enforcement and other purposes.[73] Instead of specifically delineating these law enforcement purposes, DHS grants discretion by stating that "[o]n a case-by-case basis, E-Verify may give law enforcement agencies extracts of information on potential fraud, discrimination or other illegal activities."[74] Additionally, the proposal permits broad disclosure to "Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate authority" without committing to the specific legal limitations Congress intended.[75] If executive agencies adopt E-Verify as a means of identification, the agency will have clearly contravened the express intent of Congress.

The Department should not use this SORN as an opportunity for reintroducing the costly and widely unpopular REAL ID system.

VI. Conclusion

At minimum, the agency should conduct a comprehensive overhaul and full assessment of the privacy and security implications of the program under the federal Privacy Act. Such an overhaul must entail the following rudimentary measures to begin remedying the most blatant legal and policy flaws of the current proposal.

DHS should (1) issue a new System of Records Notice limiting the agency's authority to collection, use, or disclosure of E-Verify information "for the employment eligibility purposes of the E-Verify Program or for purposes that directly support the program such as prevention of

[72] DHS Data Privacy & Integrity Advisory Committee, Comments Regarding the Notice of Proposed Rulemaking for Implementation of the REAL ID Act (May 2007), http://epic.org/privacy/id_cards/dpiac_comm_050707.pdf
[73] Department of Homeland Security Notice of Privacy Act System of Records, 76 Fed. Reg. 26, 738, 26, 741 (May 9, 2011).
[74] May 9, 2011 System of Records Notice at 26740.
[75] *Id.* at 26745..

misuse and fraud, program analysis and outreach;"[76] (2) retract all assertions of legal authority in the agency's SORN that are contrary to this commitment; (3) develop an effective system for meaningfully enforcing the right of data subjects to quickly correct inaccurate E-Verify records in compliance with the Privacy Act; (4) monitor and enforce the administrative policies the agency has developed to prevent identity theft and inaccurate government records; and (5) ensure that the proposed E-Verify expansion does not default into a national ID system analogous to REAL ID.

Precise commitments and limitations regarding the agency's proposed legal authority will give the public a better opportunity to assess and comment on the privacy, security, and economic costs of the new E-Verify program. As currently proposed, this program is contrary to law, exceeds the scope of the agency's authority, and should be withdrawn.

Sincerely,

Marc Rotenberg
EPIC Executive Director

Lillie Coney
EPIC Associate Director

Conor Kennedy
EPIC Appellate Advocacy Fellow

EPIC IPIOP 2011 Clerks:

[76] U. S. Citizenship and Immigration Services, Dept. of Homeland Security, E-Verify Program Privacy Impact Assessment 31 (May 4, 2010).

Sapna Mehta
Andrew Christy
Jeramie Scott
Alexandra Wood